[정보보호] SNS에서의 개인정보보호

트위터나 페이스북, 싸이월드와 같은 소셜 네트워크의 사용자가 급속히 늘어나면서 이런 소셜 네트워크를 통해 전달되는 개인정보나 공적 정보들이 넘쳐나고 있다. 이러한 정보의 오용이나 남용으로 법적인 잘못을 저질러 감옥에 가거나 인생을 망치게 되는 경우도 신문지상이나 뉴스에서 흔히 보도가 되곤 한다. 개인의 정보보호는 그동안 인터넷 공간의 발달과 활용으로 이미 여러 번 언급되고 그 중요성이 알려지고 있다. 그러나 이러한 SNS(Social Network Service, 이하 소셜 네트워크 서비스)에서의 개인정보보호는 중요성이 널리 홍보되지 못하고 준비되어 있지 못한 것으로 생각된다. 앞으로의 사회는 통신에서의 정보가 막대한 비중을 차지하는 세상이 될 것이나 그 정보의 올바른 사용이 전제되지 않는다면 오히려 그것은 대재앙으로 다가올 수 있을 것이다. 이러한 점에서 온라인상에서의 개인정보보호뿐만 아니라 소셜 네트워크에서의 개인정보보호도 우리가 주의 깊게 살펴보고 개인정보의 오남용을 막기 위한 노력을 경주할 때이다.

국내외 개인정보보호 침해 사례

2011년 6월 스타로 떠오르던 미국 뉴욕시의 한 의원은 3년간 인터넷을 통해 알고 지냈던 여성들에게 음란한 사진을 보냈다는 이유로 사임하였고 이로 인해 전도유망하였던 그의 정치적 미래는 송두리째 무너지고 말았는데 사적인 공간으로 여겨졌던 SNS에서의 개인정보가 외부로 알려지면서 발생한 사건이었다. 이와 비슷한 사례는 여기저기서 더 찾아볼 수 있는데 미국의 한 여교사는 인터넷 자신의 페이스북에 여행 중 음주를 하고 욕설을 담은 동영상을 올려 물의를 일으켜 결국 교사로서의 행동에 부적절하다는 여론에 떠밀려 교사직을 사임하였다. 개인의 여행지에서 개인적인 행동을 한 것이 개인적인 공간에 올려져서 벌어진 상황으로 그녀 자신은 개인 공간이라고 생각되었던 공간에서 이러한 일이 생길 거라고는 상상도 하지 못하였을 것이다. 또 다른 예로 세계적인 네트워크 업체에 입사가 예정된 상황에서 어떤 미국인이 자신의 트위터에 '회사를 미워해야 한다'는 내용의 글을 올렸다가 입사가 취소되기도 하였다. 이처럼 미국 회사 중 8%가 직원들의 잘못된 SNS 이용을 사유로 해고한다고 한다.

해킹에 의한 개인정보의 누출 위협도 심각하기는 마찬가지이다. 사실 웹 서버에서 개인의 정보를 탈취하는 데는 5분도 채 걸리지 않는데 로그인 창이나 게시판에 특정 문자열을 입력했을 때 나타나는 오류를 이용, 개인정보를 탈취하고 악성코드를 삽입하기 위한 SQL 인젝션 공격은 불과 5분 정도의 짧은 시간만이 필요할 뿐이다. 최근 SQL 인젝션 공격에 의해 어떤 한 투자증권에서는 1만 2천여 건의 개인정보를 도난 당했으며, 모 캐피탈 업체의 경우 170여 만 명의 고객 개인정보를 해킹 당한 실례가 있다. 또한, 일본의 한 기업의 경우에는 비디오게임기 플레이스테이션 시리즈의 가입자 개인정보가 해킹으로 대거 유출돼 수천 억 원 규모의 피해를 입은 것으로 추산되고 있으며, 일본의 다른 한 기업의 경우 미국 법인의 웹사이트 서버가 해킹을

당한 사실이 밝혀지기도 하였다. 이외에도 국내외 수많은 게임업계가 최근 해킹에 의한 고객 개인정보 누출 사고로 그 피해가 날로 증가되고 있는 상황이다.

최근 스마트폰 이용자가 2천만 가입자에 이를 것으로 예측되고 있다. 이러한 스마트폰과 같은 무선 단말기를 이용한 증권 거래액이 지난 5월 16일까지 74조 3천억 원에 달한 것으로 나타났다. 올 전체로는 150조원을 넘어설 것으로 예측되고 있다. 이처럼 막대한 금융 자산이 이동하고 있는 무선 인터넷은 누구나 쉽게 접근할 수 있어 정보 갈취와 해킹에 취약한 것이 사실이다. 이러한 무선랜을 이용할 경우 악성 AP(Access Point)를 통해 중간에서 개인정보를 유출시키는 일이 발생할 수 있으며, 이를 활용하여 개인의 금융자산을 공격할 경우 그 피해는 막대할 것으로 예측된다. 더욱이 스마트 기기의 분실과 도난으로 일어날 수 있는 개인정보 누출사고도 얼마든지 발생될 소지가 있는 것이다. 지난 농협 전산망 해킹에서 알 수 있듯이 금융사의 시스템 사고는 엄청난 경제적 손실뿐만 아니라 사회적 파장 또한 엄청날 것이다. 특히, 현재보다도 미래의 금융 생활에서는 절대로 빠질 수 없는 것이 스마트 금융일 것이다. 이는 스마트 기기를 활용하여 비대면 상황에서 네트워크를 통해 금융 거래를 한다는 것이다. 그런데, 이러한 금융 거래 유형에서 개인정보가 누출되어 본인이 아닌 제3자가 본인의 금융 자산을 갈취하게 된다면 미래의 스마트 금융 거래는 매우 취약해지고 사회적으로 불안감이 팽배해질 것이다. 따라서, 안전한 금융 거래 환경을 조성하기 위해서도 개인정보보호의 중요성은 더 이상 강조할 필요가 없을 것이다.

개인정보 누출로 인한 대표적인 피해에는 보이스 피싱(voice phishing) 사고를 들 수 있다. 이미 그동안 수없이 많은 사고들이 신문이나 TV 등을 통해 알려졌음에도 불구하고 이러한 보이스 피싱 사기 사건은 끊이질 않고 발생되고 있는 상황이다. 따라서 금융 소비자는 절대로 전화를 통해 계좌번호, 카드번호, 주민등록번호 등의 개인정보를 누출하지 말아야 할 것이다.

이러한 피해를 예방하기 위한 하나의 방안으로 인터넷 이용시 비실명 이메일 인증 방식을 활용하는 업체들이 늘고 있는 것은 고무적인 현상이다. 최근 스마트폰 확대로 모바일 서비스가 활성화 되면서 개인정보를 활용한 주민등록번호나 아이핀을 이용하는 실명 인증 방식에 비해 상대적으로 절차가 간편한 비실명 이메일 인증을 도입하고 있는 것이다. 이를 활용한 경우에는 불필요한 개인정보를 수집하지 않는 데다 절차가 간편하다는 장점이 있다. 물론, 우리나라의 경우에는 게시판 등에 인터넷 실명제를 적용하고 있는 곳이 많이 있지만 이 경우에도 해당되는 서비스를 활용할 때만 임시로 사용자의 실명을 확인할 수 있는 방법을 활용한다면 전체적으로 개인정보를 굳이 인터넷 업체에 저장할 필요가 없으므로 개인정보보호 측면에서는 매우 유용한 방법이라 할 것이다.

앞서 살펴본 바와 같은 개인정보 유출에 의한 사고를 미연에 방지하기 위해서는 회원가입을 하거나 개인정보를 제공할 때에는 이용약관을 꼼꼼히 살펴봐야 할 것이며, 비밀번호는 문자와 숫자를 조합하여 충분한 길이로 만들고 이를 주기적으로 변경하여야 할 것이다. 또한, P2P나 PC방과 같이 다수의 사용자들에게 노출될 수 있는 사이트를 이용할 시에는 절대로 개인정보를 저장하지 않아야 하고, 공공장소에서의 금융거래도 유의하여야 할 것이다. 마지막으로 해킹에

의한 개인정보 누출 사고를 예방하기 위해서는 무엇보다도 출처가 불명확한 자료는 사용을 금지하여야 하고 개인정보 침해사고가 발생한 때에는 적극적인 신고 정신을 발휘하는 것이 필요할 것이다

표준화 현황

이러한 소셜 네트워크에서의 개인정보보호에 대한 기고문이 2012년 7월 태국 방콕에서 열린 제20차 ASTAP forum 회의에서 발표되었으며 이 기고문을 바탕으로 ASTAP forum의 정보보호 전문가그룹에서 논의되고 있는 정보보호 핸드북을 만드는 작업에 소셜 네트워크에서의 개인정보보호를 포함하는 좀 더 광범위하고 일반적인 개인정보보호를 다루어 그 중요성을 널리 알리고 연구와 실제 적용의 필요성을 공유해야 한다는 목소리가 크다.

세계 각국에서도 자국의 개인정보보호를 위해 기술적, 정책적 연구가 이루어져 왔으며 몇몇 나라에서는 이미 법률 및 가이드라인을 제시하거나 확정하여 운영하고 있는 실정이다. OECD에서도 이미 가이드라인을 제정하여 가입 국가들에게 배포하였으며 아시아, 태평양 지역의 표준화 단체인 APT(Asia-Pacific Telecommunity)에서도 2004년 우리나라의 주도로 개인정보보호 가이드라인을 구성하여 발표한 바 있다.

지난 2005년 3월에 열린 제9차 ASTAP forum에서도 웹과 RFID에서의 개인정보보호 가이드라인 권고안을 작성하자는 한국측의 기고서가 제출된 바 있으며 이러한 노력의 결과로 개인정보보호에 대한 인식은 몇 년 전에 비해 비약적으로 발전하였다. 그러나 기존의 개인정보보호에 관한 내용이 주로 웹을 통한 통신에서의 개인정보보호였다면 이번 제20차 ASTAP forum에서의 개인정보보호는 그 내용이 소셜 네트워크로 확장된 것으로 볼 수 있다.

제20차 ASTAP forum에서는 정보보호 전문가 그룹 주도하에 정보보호 핸드북을 만들어 정보보호가 취약한 아시아, 태평양 지역 국가들을 대상으로 최신 이슈들에 대한 정보를 제공하고 이를 기반으로 해당 국가들에 대한 튜토리얼 역할과 함께 아시아, 태평양 지역의 공동 발전을 위한 마스터 플랜을 짜는 것을 추진하기로 합의되었다. 또한, 7월 태국 방콕 회의에서는 한국의 제안으로 소셜 네트워크 환경에서의 개인정보보호 중요성이 인정되어, 본 핸드북에 일반적인 개인정보보호를 다룰 수 있는 독립적인 목차의 하나로 추후 작업을 준비해 나가기로 합의를 하였다. 이러한 작업을 위해서는 정부의 역할도 중요하며 개인정보를 처리하거나 제한을 두는 행위, 표현의 자유와의 관계 등도 고려하여 특정 매체나 도구만을 고려하지 않는 범용적인 가이드라인 제시도 함께 필요한 상황이다.

이러한 개인정보보호에 관한 내용은 국제전기통신연합(ITU: International Telecommunication Union)의 권고안으로도 아직까지 제시되지 않아 아시아, 태평양을 넘어 세계의 모든 나라에 도움이 되는 가이드라인이 필요한 상황이다. 우리나라에서도 이러한 정보보호 핸드북 작성에 적극적으로 협조하여 우리나라를 넘어 세계적으로 개인정보보호 공조 체계를 구축하고 우리의 소중한 정보를 보호하는 데에 앞장서야 할 것이다.

류희수 (경인교육대학교 수학교육과 교수, hsryu@ginue.ac.kr)